

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-283320
(P2001-283320A)

(43) 公開日 平成13年10月12日 (2001.10.12)

(51) Int.Cl. ⁷	識別記号	F I	テームト [*] (参考)
G 0 7 F 17/00		G 0 7 F 17/00	B 5 B 0 4 9
G 0 6 F 17/60	3 0 2	G 0 6 F 17/60	3 0 2 E 5 C 0 6 4
	5 1 2		5 1 2 5 D 0 4 4
G 1 0 K 15/02		G 1 0 K 15/02	5 J 1 0 4
G 1 1 B 20/10		G 1 1 B 20/10	H
審査請求 未請求 請求項の数 8 O L (全 15 頁) 最終頁に続く			

(21) 出願番号 特願2000-96883 (P2000-96883)

(22) 出願日 平成12年3月31日 (2000.3.31)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 岸 治彦

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 栗原 章

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

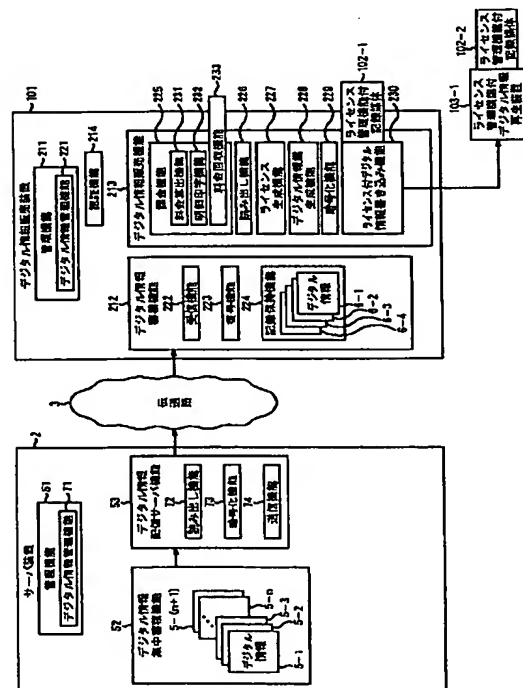
最終頁に続く

(54) 【発明の名称】 情報販売装置および方法、並びにプログラム格納媒体

(57) 【要約】

【課題】 販売した情報の不正な利用を防止する。

【解決手段】 デジタル情報蓄積機能212は、販売するデジタル情報6を蓄積する。ライセンス生成機能227は、デジタル情報6に対応する利用条件を生成する。暗号化機能229は、デジタル情報6を暗号化する。デジタル情報鍵生成機能228は、暗号化されたデジタル情報6を復号する暗号鍵を生成する。認証機能214は、デジタル情報販売装置101に装着されているライセンス管理機能付記録媒体102-1を認証する。ライセンス付デジタル情報書き込み機能230は、認証されたライセンス管理機能付記録媒体102-1に、暗号化されたデジタル情報6を利用条件および暗号鍵と共に書き込む。



【特許請求の範囲】

【請求項 1】 販売する情報を蓄積する蓄積手段と、前記情報に対応する利用条件を生成する利用条件生成手段と、前記情報を暗号化する暗号化手段と、暗号化された前記情報を復号する暗号鍵を生成する暗号鍵生成手段と、自分自身に装着されている記録媒体を認証する認証手段と、前記認証手段により認証された前記記録媒体に、暗号化された前記情報を前記利用条件および前記暗号鍵と共に書き込む書き込み手段とを含むことを特徴とする情報販売装置。

【請求項 2】 前記記録媒体に記録されている前記情報を再生する再生装置と通信する通信手段を更に含み、前記認証手段は、前記通信手段が前記再生装置と通信するとき、前記再生装置を更に認証し、前記書き込み手段は、前記再生装置を介して、前記記録媒体に、暗号化されている前記情報を前記利用条件および前記暗号鍵と共に書き込むことを特徴とする請求項 1 に記載の情報販売装置。

【請求項 3】 前記通信手段は、前記再生装置に一体的に設けられている前記記録媒体に記録されている前記情報を再生する再生装置と通信し、前記書き込み手段は、前記再生装置に一体的に設けられている前記記録媒体に、暗号化されている前記情報を前記利用条件および前記暗号鍵と共に書き込むことを特徴とする請求項 2 に記載の情報販売装置。

【請求項 4】 所定の伝送路を介して送信された前記情報を受信する受信手段を更に含み、前記蓄積手段は、前記受信手段が受信した前記情報を蓄積することを特徴とする請求項 1 に記載の情報販売装置。

【請求項 5】 前記利用条件生成手段は、前記記録媒体に記録されている前記情報を再生する再生装置が従う前記利用条件を生成し、前記暗号化手段は、前記再生装置が復号可能な方式で前記情報を暗号化することを特徴とする請求項 1 に記載の情報販売装置。

【請求項 6】 前記情報は、プログラム、音声、音楽、静止画像、動画像、およびテキストの少なくとも 1 つを含むことを特徴とする請求項 1 に記載の情報販売装置。

【請求項 7】 販売する情報を蓄積する蓄積ステップと、前記情報に対応する利用条件を生成する利用条件生成ステップと、前記情報を暗号化する暗号化ステップと、暗号化された前記情報を復号する暗号鍵を生成する暗号鍵生成ステップと、装着されている記録媒体を認証する認証ステップと、

前記認証ステップの処理で認証された前記記録媒体に、暗号化された前記情報を前記利用条件および前記暗号鍵と共に書き込む書き込みステップとを含むことを特徴とする情報販売方法。

【請求項 8】 販売する情報を蓄積する蓄積ステップと、前記情報に対応する利用条件を生成する利用条件生成ステップと、前記情報を暗号化する暗号化ステップと、暗号化された前記情報を復号する暗号鍵を生成する暗号鍵生成ステップと、装着されている記録媒体を認証する認証ステップと、前記認証ステップの処理で認証された前記記録媒体に、暗号化された前記情報を前記利用条件および前記暗号鍵と共に書き込む書き込みステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報販売装置および方法、並びにプログラム格納媒体に関し、特に、音楽のデータなどの情報を販売する情報販売装置および方法、並びにプログラム格納媒体に関する。

【0002】

【従来の技術】図 1 は、従来のデジタル情報販売システムの構成を説明する図である。デジタル情報販売装置 1 は、販売店（いわゆる、コンビニエンスストアなど）の店頭などに設置され、伝送路 3 を介して、サーバ装置 2 から送信されたデジタル情報を受信して、その内部に記録する。デジタル情報販売装置 1 は、その内部に記録しているデジタル情報を販売するとき、購入者が所有する記録媒体 4 が装着され、装着されている記録媒体 4 にデジタル情報を記録させる。

【0003】デジタル情報販売装置 1 は、管理機能 11、デジタル情報蓄積機能 12、およびデジタル情報販売機能 13 を有する。管理機能 11 は、デジタル情報管理機能 21 を有し、デジタル情報蓄積機能 12 およびデジタル情報販売機能 13 を制御する。

【0004】デジタル情報蓄積機能 12 は、受信機能 22、復号機能 23、および記録保持機能 24 から構成される。受信機能 22 は、伝送路 3 を介して、サーバ装置 2 から送信された暗号化されているデジタル情報を受信して、復号機能 23 に供給する。

【0005】復号機能 23 は、予め、鍵を記憶し、復号機能 23 から供給された、暗号化されているデジタル情報を復号する。記録保持機能 24 は、復号機能 23 から供給された、復号されたデジタル情報を、デジタル情報 6-1 乃至 6-4 として記録する。

【0006】デジタル情報販売機能 13 は、課金機能 25、読み出し機能 26、および書き込み機能 27 から構

成される。

【0007】課金機能25は、デジタル情報蓄積機能12に記録されているデジタル情報6-1乃至6-4を販売するとき、購入者から料金を徴収する。課金機能25は、更に、料金算出機能31、明細印字機能32、および料金回収機能33から構成される。

【0008】料金算出機能31は、販売するデジタル情報6-1乃至6-4の価格を算出する。明細印字機能32は、デジタル情報6-1乃至6-4を販売するとき、領収書に販売価格などを印刷して出力する。

【0009】料金回収機能33は、購入者により挿入された代金に対応する貨幣から、販売するデジタル情報6-1乃至6-4の価格に対応する料金を回収する。

【0010】読み出し機能26は、販売するデジタル情報6-1乃至6-4の価格に対応する料金が支払われたとき、購入者の選択に基づいて、デジタル情報蓄積機能12が蓄積しているデジタル情報6-1乃至6-4のいずれかを読み出して、読み出したデジタル情報6-1乃至6-4のいずれかを書き込み機能27に供給する。

【0011】書き込み機能27は、読み出し機能26から供給されたデジタル情報6-1乃至6-4のいずれかを、装着されている記録媒体4に書き込む。

【0012】以下、デジタル情報6-1乃至6-4を個々に区別する必要がないとき、単に、デジタル情報6と称する。

【0013】サーバ装置2は、予め定めた時刻（例えば、毎日の午前0時）に、予め記録しているデジタル情報5-1乃至5-(n+1)の中からデジタル情報販売装置1に送信するものを選択して、選択したデジタル情報5-1乃至5-(n+1)のいずれかを、伝送路3を介して、デジタル情報販売装置1に送信する。

【0014】サーバ装置2は、管理機能51、デジタル情報集中蓄積機能52、およびデジタル情報配信サーバ機能53を有する。管理機能51は、デジタル情報管理機能71を有し、デジタル情報集中蓄積機能52およびデジタル情報配信サーバ機能53を制御する。

【0015】デジタル情報集中蓄積機能52は、デジタル情報販売装置1に送信するためのデジタル情報5-1乃至5-(n+1)を蓄積する。

【0016】デジタル情報配信サーバ機能53は、デジタル情報集中蓄積機能52から蓄積されているデジタル情報5-1乃至5-(n+1)を読み出して、暗号化して、伝送路3を介して、デジタル情報販売装置1に送信する。デジタル情報配信サーバ機能53は、読み出し機能72、暗号化機能73、および送信機能74を有する。

【0017】読み出し機能72は、デジタル情報集中蓄積機能52から蓄積されているデジタル情報5-1乃至5-(n+1)のいずれかを読み出して、暗号化機能73に供給する。暗号化機能73は、読み出し機能72か

ら供給されたデジタル情報5-1乃至5-(n+1)のいずれかを、DES (Data Encryption Standard) などの方式で暗号化して、送信機能74に供給する。送信機能74は、暗号化されたデジタル情報5-1乃至5-(n+1)のいずれかを、伝送路3を介して、デジタル情報販売装置1に送信する。

【0018】以下、デジタル情報5-1乃至5-(n+1)を個々に区別する必要がないとき、単にデジタル情報5と称する。

10 【0019】【発明が解決しようとする課題】しかしながら、記録媒体4には、不正なコピーまたは再生など、本来許可されていない利用を防止する機能が無く、また、デジタル情報6に対応する利用条件等も記録媒体4に記録されないため、販売されたデジタル情報について、不正な利用を防止することができないという問題点があった。

【0020】本発明はこのような状況に鑑みてなされたものであり、販売した情報の不正な利用の防止ができるようにすることを目的とする。

20 【0021】【課題を解決するための手段】請求項1に記載の情報販売装置は、販売する情報を蓄積する蓄積手段と、情報に対応する利用条件を生成する利用条件生成手段と、情報を暗号化する暗号化手段と、暗号化された情報を復号する暗号鍵を生成する暗号鍵生成手段と、自分自身に装着されている記録媒体を認証する認証手段と、認証手段により認証された記録媒体に、暗号化された情報を利用条件および暗号鍵と共に書き込む書き込み手段とを含むことを特徴とする。

30 【0022】情報販売装置は、記録媒体に記録されている情報を再生する再生装置と通信する通信手段を更に設け、認証手段が、通信手段が再生装置と通信するとき、再生装置を更に認証し、書き込み手段が、再生装置を介して、記録媒体に、暗号化されている情報を利用条件および暗号鍵と共に書き込むようにすることができる。

【0023】通信手段は、再生装置に一体的に設けられている記録媒体に記録されている情報を再生する再生装置と通信し、書き込み手段は、再生装置に一体的に設けられている記録媒体に、暗号化されている情報を利用条件および暗号鍵と共に書き込むようにすることができる。

40 【0024】情報販売装置は、所定の伝送路を介して送信された情報を受信する受信手段を更に設け、蓄積手段が、受信手段が受信した情報を蓄積するようにすることができる。

【0025】利用条件生成手段は、記録媒体に記録されている情報を再生する再生装置が従う利用条件を生成し、暗号化手段は、再生装置が復号可能な方式で情報を暗号化するようにすることができる。

50 【0026】情報は、プログラム、音声、音楽、静止画

像、動画像、およびテキストの少なくとも1つを含むようにすることができる。

【0027】請求項7に記載の情報販売方法は、販売する情報を蓄積する蓄積ステップと、情報に対応する利用条件を生成する利用条件生成ステップと、情報を暗号化する暗号化ステップと、暗号化された情報を復号する暗号鍵を生成する暗号鍵生成ステップと、装着されている記録媒体を認証する認証ステップと、認証ステップの処理で認証された記録媒体に、暗号化された情報を利用条件および暗号鍵と共に書き込む書き込みステップとを含むことを特徴とする。

【0028】請求項8に記載のプログラム格納媒体のプログラムは、販売する情報を蓄積する蓄積ステップと、情報に対応する利用条件を生成する利用条件生成ステップと、情報を暗号化する暗号化ステップと、暗号化された情報を復号する暗号鍵を生成する暗号鍵生成ステップと、装着されている記録媒体を認証する認証ステップと、認証ステップの処理で認証された記録媒体に、暗号化された情報を利用条件および暗号鍵と共に書き込む書き込みステップとを含むことを特徴とする。

【0029】請求項1に記載の情報販売装置、請求項7に記載の情報販売方法、および請求項8に記載のプログラム格納媒体においては、販売する情報が蓄積され、情報に対応する利用条件が生成され、情報が暗号化され、暗号化された情報を復号する暗号鍵が生成され、装着されている記録媒体が認証され、認証された記録媒体に、暗号化された情報が利用条件および暗号鍵と共に書き込まれる。

【0030】

【発明の実施の形態】図2は、本発明に係るデジタル情報販売システムの一実施の形態を説明する図である。デジタル情報販売装置101は、販売店（いわゆる、コンビニエンスストアなど）の店頭などに設置され、伝送路3を介して、サーバ装置2から送信されたデジタル情報（プログラム、またはテキスト、楽音を含む音楽、音声、若しくは静止画像、動画像のデータなど）を受信して、その内部に記録する。

【0031】デジタル情報販売装置101は、例えば、音楽データであるデジタル情報を販売する場合、SDMI (Secure Digital Music Initiative) の規格に準拠して、デジタル情報に対応する利用条件を生成すると共に暗号鍵（以下、デジタル情報鍵と称する）を生成して、デジタル情報をデジタル情報鍵で復号できるように暗号化して、デジタル情報を利用条件およびデジタル情報鍵と共に、ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1に供給する。

【0032】デジタル情報販売装置101は、DESなどの共通鍵暗号方式で、デジタル情報を暗号化するとき、デジタル情報鍵でデジタル情報を暗号化する。デジタル

情報販売装置101は、RSA (Rivest-Shamir-Adleman) などの公開鍵暗号方式で、デジタル情報を暗号化するとき、秘密鍵でデジタル情報を暗号化して、公開鍵をデジタル情報鍵として、ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1に供給する。

【0033】例えば、音楽データであるデジタル情報を利用する場合、ライセンス管理機能付デジタル情報再生装置103-1および103-2、パーソナルコンピュータ104、並びに携帯端末装置105は、SDMIの規格に準拠したソフトウェアモジュールであるLCM (Licensed Compliant Module) を有し、デジタル情報に対応する利用条件に基づいて、デジタル情報の、例えば、いわゆる、チェックイン、チェックアウト、コピー、または移動などを許可するか、または禁止する。

【0034】ライセンス管理機能付記録媒体102-1および102-2は、デジタル情報に対応する利用条件に基づいて、記録しているデジタル情報の利用を管理する（例えば、読み出しを許可または禁止する）。

【0035】伝送路3は、有線または無線の通信路であり、例えば、専用線、LAN (Local Area Network)、ISDN (Integrated Services Digital Network)、xDSL (x Digital Subscriber Line)、電話回線、PHS (Personal Handyphone System) 回線、携帯電話回線、WLL (Wireless Local Loop) 回線、通信衛星回線、または放送衛星回線などである。

【0036】デジタル情報販売装置101は、その内部に記録しているデジタル情報6を購入するために、購入者が所有するライセンス管理機能付記録媒体102-1が装着部111に装着されたとき、ライセンス管理機能付記録媒体102-1との相互認証の処理を実行する。デジタル情報販売装置101は、デジタル情報6に対応する利用条件を生成するとともに、デジタル情報6を暗号化して、デジタル情報6を復号するデジタル情報鍵を生成する。

【0037】デジタル情報販売装置101は、認証されたライセンス管理機能付記録媒体102-1に暗号化されているデジタル情報6を、利用条件およびデジタル情報鍵と共に記録させる。

【0038】デジタル情報販売装置101によりデジタル情報6が記録されたライセンス管理機能付記録媒体102-1は、例えば、ライセンス管理機能付デジタル情報再生機能114を有する、例えば、PDA (Personal Digital Assistant)、または携帯電話機などの携帯端末装置105に装着される。携帯端末装置105のライセンス管理機能付デジタル情報再生機能114は、ライセンス管理機能付記録媒体102-1に記録されたデジタル情報6を読み出して、そのデジタル情報6に対応する利用条件に基づき、読み出したデジタル情報6を利用することができる。

【0039】購入者が所有するライセンス管理機能付記録媒体102-2が装着されているライセンス管理機能付デジタル情報再生装置103-1のインターフェース113-1は、例えば、インターフェース113-1およびインターフェース112の通信方式に対応するケーブル等を介して、デジタル情報販売装置101のインターフェース112と接続される。デジタル情報販売装置101は、ライセンス管理機能付デジタル情報再生装置103-1が接続されたとき、ライセンス管理機能付デジタル情報再生装置103-1との相互認証の処理を実行する。

【0040】なお、ライセンス管理機能付デジタル情報再生装置103-1は、ライセンス管理機能付記録媒体102-2が装着されたとき、ライセンス管理機能付記録媒体102-2との相互認証の処理を実行する。

【0041】デジタル情報販売装置101は、認証されたライセンス管理機能付デジタル情報再生装置103-1に装着されているライセンス管理機能付記録媒体102-2に、ライセンス管理機能付デジタル情報再生装置103-1を介して、デジタル情報6を利用条件およびデジタル情報鍵と共に記録させる。

【0042】また、ライセンス管理機能付デジタル情報再生装置103-1は、その内部に一体的に設けられた記憶部に、デジタル情報販売装置101から供給されたデジタル情報6を、利用条件およびデジタル情報鍵と共に記憶させるようにしてもよい。

【0043】デジタル情報販売装置101によりデジタル情報6が記録されたライセンス管理機能付記録媒体102-2は、例えば、インターフェース113-2およびインターフェース114を介して、パーソナルコンピュータ104に接続されているライセンス管理機能付デジタル情報再生装置103-2に装着される。ライセンス管理機能付デジタル情報再生装置103-2は、そのデジタル情報6に対応する利用条件に基づき、ライセンス管理機能付記録媒体102-2に記録されたデジタル情報6を読み出して、読み出したデジタル情報6を利用することができる。

【0044】ライセンス管理機能付記録媒体102-1または102-2は、例えば、フラッシュメモリなどの半導体メモリ、フロッピー（登録商標）ディスクなどの磁気ディスク、コンパクトディスク（商標）などの光ディスク、またはミニディスク（商標）などの光磁気ディスクなどで構成される。

【0045】また、パーソナルコンピュータ104は、そのデジタル情報6に対応する利用条件に基づき、ライセンス管理機能付デジタル情報再生装置103-2を介して、ライセンス管理機能付記録媒体102-2に記録されたデジタル情報6を読み出して、読み出したデジタル情報6を利用することができる。

【0046】なお、インターフェース112、インター

フェース113-1および113-2、並びにインターフェース114は、USB (Universal Serial Bus)、IEEE (Institute of Electrical and Electronics Engineers) 1394、若しくはSCSI (Small Computer System Interface) などの有線の通信方式、またはIrDA (Infrared Data Association) が定める赤外線通信、若しくはBluetoothなどの無線の通信方式を利用することができる。

【0047】図3は、デジタル情報販売装置101の構成の例を説明する図である。CPU (Central Processing Unit) 121は、各種アプリケーションプログラムや、OS (Operating System) などを実際に実行する。ROM (Read-only Memory) 122は、一般的には、CPU 121が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random-Access Memory) 123は、CPU 121の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。

【0048】入力部125は、表示部126上に設けられたタッチパッド、または入力キーなどから構成され、CPU 121に各種の指令を入力するとき、購入者により操作される。表示部126は、液晶表示装置またはCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。音声再生部127は、例えば、CPU 121から供給されたデジタル情報6に含まれる音楽のデータなどを基に、音声を出力する。

【0049】通信部128は、伝送路3を介して、サーバ装置2から送信されたパケットに格納されているデジタル情報などのデータをCPU 121、RAM 123、または記録部129に出力する。

【0050】記録部129は、HDD (Hard Disk Drive) などで構成され、それらにCPU 121によって実行するプログラムやデジタル情報6を記録または再生させる。

【0051】ドライブ53は、装着されている磁気ディスク61、光ディスク62、光磁気ディスク63、または半導体メモリ64に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース130、およびバス124を介して接続されているRAM 123に供給する。

【0052】書き込み部131は、装着部111に装着されているライセンス管理機能付記録媒体102-1に、記録部129に記録されているデジタル情報6を書き込む。

【0053】インターフェース112は、所定の通信方式に対応するケーブルの一端が接続され、そのケーブルの他の一端に接続されているライセンス管理機能付デジタル情報再生装置103-1に、記録部129に記録されているデジタル情報6を送信する。

【0054】料金回収部132は、購入者により貨幣が投入され、貨幣が投入されたか否かを示す信号、および

投入された貨幣の額に対応する信号をCPU121に供給する。

【0055】これらのCPU121乃至料金回収部132は、バス124により相互に接続されている。

【0056】図4は、本発明に係るデジタル情報販売システムの一実施の形態の構成を説明する図である。図1に示す場合と同様の部分には、同一の番号を付してあり、その説明は省略する。

【0057】デジタル情報販売装置101は、例えば、CPU121の所定のプログラムの実行により実現される、管理機能211、デジタル情報蓄積機能212、デジタル情報販売機能213、および認証機能214を有する。管理機能211は、デジタル情報管理機能221を有し、例えば、購入者の操作に対応した入力部125の信号を基に、デジタル情報蓄積機能212およびデジタル情報販売機能213を制御する。

【0058】デジタル情報蓄積機能212は、受信機能222、復号機能223、および記録保持機能224から構成される。受信機能222は、伝送路3を介して、サーバ装置2から送信された、暗号化されているデジタル情報5を受信して、復号機能223に供給する。

【0059】復号機能223は、予め鍵を記憶し、復号機能223から供給された、暗号化されているデジタル情報5を復号する。記録保持機能224は、復号機能223から復号されたデジタル情報5を受信して、例えば、デジタル情報6-1乃至6-4として記録する。

【0060】デジタル情報販売機能213は、課金機能225、読み出し機能226、ライセンス生成機能227、デジタル情報鍵生成機能228、暗号化機能229、およびライセンス付デジタル情報書き込み機能230から構成される。

【0061】課金機能225は、デジタル情報蓄積機能212が蓄積しているデジタル情報6-1乃至6-4を販売するとき、購入者から販売するデジタル情報6-1乃至6-4の価格に対応する料金を徴収する。課金機能225は、更に、料金算出機能231、明細印字機能232、および料金回収機能233から構成される。

【0062】料金算出機能231は、販売するデジタル情報6-1乃至6-4の価格を算出する。明細印字機能232は、デジタル情報6-1乃至6-4を販売するとき、領収書などに販売価格または販売価格に対応するバーコードなどを印刷して出力する。

【0063】料金回収機能233は、料金回収部132の信号を基に、販売するデジタル情報6-1乃至6-4の価格に対応する料金を料金回収部132に回収させる。

【0064】読み出し機能226は、販売するデジタル情報6-1乃至6-4の価格に対応する料金が支払われたとき、購入者の選択に対応する、デジタル情報蓄積機能212が蓄積しているデジタル情報6-1乃至6-4

のいずれかを読み出して、読み出したデジタル情報6-1乃至6-4を暗号化機能230に供給する。

【0065】ライセンス生成機能227は、購入者の操作に対応した入力部125からの信号などに基づいて、販売するデジタル情報6-1乃至6-4のそれぞれに対応する利用条件を生成して、ライセンス付デジタル情報書き込み機能230に供給する。

【0066】デジタル情報鍵生成機能228は、販売するデジタル情報6-1乃至6-4のそれぞれに対応するデジタル情報鍵を生成して、暗号化機能229に供給する。

【0067】暗号化機能229は、デジタル情報鍵生成機能228から供給されたデジタル情報鍵で復号できるように、読み出し機能226から供給されたデジタル情報6-1乃至6-4のそれぞれを暗号化する。暗号化機能229は、対応する利用条件と共に、デジタル情報6-1乃至6-4のそれぞれを暗号化するようにしてもよい。暗号化機能229は、暗号化したデジタル情報6-1乃至6-4を、デジタル情報鍵と共にライセンス付デジタル情報書き込み機能230に供給する。

【0068】ライセンス付デジタル情報書き込み機能230は、暗号化機能229から供給されたデジタル情報6-1乃至6-4を、デジタル情報鍵および利用条件と共に、認証されたライセンス管理機能付記録媒体102-1に書き込む。また、ライセンス付デジタル情報書き込み機能230は、ライセンス管理機能付記録媒体102-2が装着されているライセンス管理機能付デジタル情報再生装置103-1に、暗号化されたデジタル情報6-1乃至6-4を、デジタル情報鍵および利用条件と共に書き込む。

【0069】ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1に供給されるデジタル情報6は、図5に示すように、デジタル情報6に対応する利用条件およびデジタル情報6を復号するためのデジタル情報鍵と対応付けられている。ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1は、デジタル情報6を利用するとき、デジタル情報鍵でデジタル情報6を復号して、対応する利用条件に基づき、デジタル情報6を利用する。

【0070】例えば、利用条件において、対応するデジタル情報6の移動は許可されているが、コピーは許可されていないとき、ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1は、そのデジタル情報6を移動させるが、そのデジタル情報6を他の機器にコピーさせない。

【0071】認証機能214は、後述する処理により、装着されたライセンス管理機能付記録媒体102-1、またはライセンス管理機能付記録媒体102-2が装着されているライセンス管理機能付デジタル情報再生装置

103-2 (接続されている) を認証する。

【0072】なお、管理機能211、デジタル情報蓄積機能212、デジタル情報販売機能213、および認証機能214は、それぞれ、専用のハードウェアで構成するようにしてもよい。

【0073】次に、購入者の所有するライセンス管理機能付記録媒体102-1にデジタル情報6を書き込んでデジタル情報6を販売するときの、デジタル情報販売装置101のデジタル情報6の販売の処理を、図6のフローチャートを参照して説明する。ステップS11において、管理機能211は、書き込み部131から供給される信号を基に、ライセンス管理機能付記録媒体102-1がデジタル情報販売装置101の装着部111に装着されたか否かを判定し、ライセンス管理機能付記録媒体102-1が装着部111に装着されていないと判定された場合、ライセンス管理機能付記録媒体102-1が装着されるまで、ステップS11の判定の処理を繰り返す。

【0074】ステップS11において、ライセンス管理機能付記録媒体102-1が装着部111に装着されたと判定された場合、ステップS12に進み、認証機能214は、装着部111に装着されているライセンス管理機能付記録媒体102-1との認証の処理を実行する。

【0075】図7は、デジタル情報販売装置101の認証機能214とライセンス管理機能付記録媒体102-1との認証の処理を説明する図である。デジタル情報販売装置101の認証機能214とライセンス管理機能付記録媒体102-1との認証の処理は、例えば、チャレンジレスポンス方式で行われる。

【0076】デジタル情報販売装置101は、予め、鍵Kabおよび自分自身のIDを記録している。ライセンス管理機能付記録媒体102-1は、予め、鍵K' (複数の鍵から構成される) を記録している。

【0077】デジタル情報販売装置101の認証機能214は、内部の乱数生成部で、乱数Naおよび乱数#Gを生成して、IDと共に、乱数Naおよび乱数#Gをライセンス管理機能付記録媒体102-1に送信する。

【0078】ライセンス管理機能付記録媒体102-1は、内部の乱数生成部で、乱数Nbおよび乱数Sbを生成する。ライセンス管理機能付記録媒体102-1は、デジタル情報販売装置101から送信された、デジタル情報販売装置101のID、乱数Na、および乱数#Gを受信する。ライセンス管理機能付記録媒体102-1の算出部は、乱数#Gに所定の関数を適用して、変数jを生成する。

【0079】ライセンス管理機能付記録媒体102-1の算出部は、変数jを基に、複数の鍵から構成される鍵K'の中から所定の鍵K'_jを選択して、選択した鍵K'_jを鍵として、デジタル情報販売装置101のIDにハッシュ関数を適用して、鍵Kabを求める。

【0080】ライセンス管理機能付記録媒体102-1の算出部は、鍵Kabを鍵として、デジタル情報販売装置101から受信した乱数Na、生成した乱数Nb、およびデジタル情報販売装置101のIDにハッシュ関数を適用して、変数Rを算出する。

【0081】ライセンス管理機能付記録媒体102-1は、乱数Nb、変数R、変数j、および乱数Sbをデジタル情報販売装置101に送信する。

【0082】デジタル情報販売装置101は、ライセンス管理機能付記録媒体102-1が送信した、乱数Nb、変数R、変数j、および乱数Sbを受信する。

【0083】デジタル情報販売装置101の認証機能214は、鍵Kabを鍵として、乱数Na、ライセンス管理機能付記録媒体102-1から受信した乱数Nb、および自分自身のIDにハッシュ関数を適用して算出された値が、ライセンス管理機能付記録媒体102-1から受信した変数Rと等しいか否かを判定し、鍵Kabを鍵として、乱数Na、乱数Nb、およびIDにハッシュ関数を適用して算出された値が変数Rと等しいと判定された場合、ライセンス管理機能付記録媒体102-1を正当であると認証する。

【0084】鍵Kabを鍵として、乱数Na、乱数Nb、およびIDにハッシュ関数を適用して算出された値が変数Rと等しくない判定された場合、デジタル情報販売装置101の認証機能214は、ライセンス管理機能付記録媒体102-1が正当でないと判定し、ライセンス管理機能付記録媒体102-1を認証せず、処理は終了する。

【0085】ライセンス管理機能付記録媒体102-1を正当であると認証された場合、デジタル情報販売装置101の認証機能214は、鍵Kabを鍵として、乱数Nbおよび乱数Naにハッシュ関数を適用して、変数R'を算出する。デジタル情報販売装置101の認証機能214は、鍵Kabを鍵として、乱数Saおよび乱数Sbにハッシュ関数を適用して、一時鍵Ksを算出する。

【0086】デジタル情報販売装置101の認証機能214は、変数R'および乱数Saをライセンス管理機能付記録媒体102-1に送信する。

【0087】ライセンス管理機能付記録媒体102-1は、デジタル情報販売装置101から送信された変数R'および乱数Saを受信する。

【0088】ライセンス管理機能付記録媒体102-1は、鍵Kabを鍵として、乱数Nb、および乱数Naにハッシュ関数を適用して算出された値が、ライセンス管理機能付記録媒体102-1から受信した変数R'と等しいか否かを判定し、鍵Kabを鍵として、乱数Nb、および乱数Naにハッシュ関数を適用して算出された値が、変数R'と等しいと判定された場合、デジタル情報販売装置101を正当であると認証する。

【0089】鍵Kabを鍵として、乱数Nb、および乱数Naにハッシュ関数を適用して算出された値が、変数R'と等くないと判定された場合、ライセンス管理機能付記録媒体102-1は、デジタル情報販売装置101が正当でないと判定し、デジタル情報販売装置101を認証せず、処理は終了する。

【0090】デジタル情報販売装置101が正当であると認証された場合、ライセンス管理機能付記録媒体102-1は、鍵Kabを鍵として、乱数Saおよび乱数Sbにハッシュ関数を適用して、一時鍵Ksを算出する。

【0091】このように、デジタル情報販売装置101とライセンス管理機能付記録媒体102-1とは、相互認証すると共に、相互認証されたとき、共通の一時鍵Ksを共有する。

【0092】なお、認証の処理で利用されるハッシュ関数として、DESを利用するようにしてもよい。

【0093】ステップS13において、管理機能211は、ステップS12の処理でライセンス管理機能付記録媒体102-1が認証されたか否かを判定し、ライセンス管理機能付記録媒体102-1が認証されたと判定された場合、ステップS14に進み、デジタル情報蓄積機能212から供給されるデータを基に、表示部126に、販売可能なデジタル情報6の選択画面を表示させる。

【0094】ステップS15において、管理機能211は、購入者の操作に対応した入力部125からの信号を基に、販売するデジタル情報6が決定されたか否かを判定し、販売するデジタル情報6が決定されたと判定された場合、ステップS16に進み、デジタル情報販売機能213の料金算出機能231に、販売するデジタル情報6の価格を算出させる。

【0095】ステップS17において、管理機能211は、デジタル情報販売機能213の料金回収部132からの信号を基に、料金回収部132に代金が投入されたか否かを判定し、料金回収部132に代金が投入されたと判定された場合、ステップS18に進み、料金回収部132に投入された代金を料金回収機能233に数えさせる。

【0096】ステップS19において、管理機能211は、ステップS16で算出されたデジタル情報6の価格、および料金回収機能233から供給された、料金回収部132に投入された代金に対応する信号を基に、投入された代金でデジタル情報6が販売できるか否かを判定し、投入された代金でデジタル情報6が販売できると判定された場合、ステップS20に進み、読み出し機能226に、記録保持機能224から所定のデジタル情報6を読み出させる。ライセンス生成機能227は、読み出したデジタル情報6に対応する利用条件を生成する。デジタル情報鍵生成機能228は、デジタル情報6を復号するデジタル情報鍵を生成する。暗号化機能229

は、例えば、DESの方式で、デジタル情報6を暗号化する。

【0097】ライセンス付デジタル情報書き込み機能230は、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体102-1にデジタル情報6を記録する。

【0098】ステップS21において、管理機能211は、書き込み部131、またはライセンス付デジタル情報書き込み機能230から供給される信号を基に、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体102-1にデジタル情報6が正常に記録されたか否かを判定し、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体102-1にデジタル情報6が正常に記録されたと判定された場合、ステップS22に進み、デジタル情報販売装置101の装着部111からライセンス管理機能付記録媒体102-1を排出させ、処理は終了する。

【0099】ステップS13において、ライセンス管理機能付記録媒体102-1が認証されないと判定された場合、ライセンス管理機能付記録媒体102-1が正当ではないので、ステップS23に進み、管理機能211は、表示部126に認証されなかった旨を示すエラーメッセージを表示させ、処理は終了する。

【0100】ステップS15において、販売するデジタル情報6が決定されず、処理の中止が要求されたと判定された場合、ステップS24に進み、管理機能211は、表示部126に処理が中断された旨を示すメッセージを表示させ、処理は終了する。

【0101】ステップS17において、料金回収部132に代金が投入されず、処理の中止が要求されたと判定された場合、ステップS25に進み、管理機能211は、表示部126に処理が中断された旨を示すメッセージを表示させ、処理は終了する。

【0102】ステップS19において、投入された代金でデジタル情報6が販売できないと判定された場合、ステップS26に進み、管理機能211は、表示部126に、代金が足りないので処理が中断された旨を示すメッセージを表示させ、料金回収部132に投入された代金を排出させて、処理は終了する。

【0103】ステップS21において、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体102-1にデジタル情報6が正常に記録されないと判定された場合、ステップS27に進み、管理機能211は、表示部126に、書き込みが失敗した旨を示すエラーメッセージを表示させ、処理は終了する。

【0104】以上のように、デジタル情報販売装置101は、ライセンス管理機能付記録媒体102-1に、デジタル情報鍵および利用条件と共に、デジタル情報6を記録させることができる。

【0105】なお、デジタル情報販売装置101は、同

様の処理で、ライセンス管理機能付記録媒体 102-2 が装着されているライセンス管理機能付デジタル情報再生装置 103-1 に、デジタル情報鍵および利用条件と共にデジタル情報 6 を書き込む。

【0106】次に、購入者の所有するライセンス管理機能付記録媒体 102-1 にデジタル情報 6 を書き込んでデジタル情報 6 を販売するときの、デジタル情報販売装置 101 のデジタル情報 6 の販売の他の処理を、図 8 のフローチャートを参照して説明する。ステップ S 51 乃至ステップ S 55 の処理は、図 6 のステップ S 11 乃至ステップ S 15 の処理と、それぞれ同様であるので、その説明は省略する。

【0107】ステップ S 55 において、販売するデジタル情報 6 が決定されたと判定された場合、ステップ S 56 に進み、管理機能 11 は、読み出し機能 226 に、記録保持機能 224 から販売が決定されたデジタル情報 6 を読み出させる。ライセンス生成機能 227 は、読み出したデジタル情報 6 に対応する利用条件を生成する。デジタル情報鍵生成機能 228 は、デジタル情報 6 を復号するデジタル情報鍵を生成する。暗号化機能 229 は、

例えば、DES の方式で、デジタル情報 6 を暗号化する。

【0108】ライセンス付デジタル情報書き込み機能 230 は、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 102-1 にデジタル情報 6 を記録する。

【0109】ステップ S 57 において、管理機能 211 は、書き込み部 131、またはライセンス付デジタル情報書き込み機能 230 から供給される信号を基に、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 102-1 にデジタル情報 6 が正常に記録されたか否かを判定し、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 102-1 にデジタル情報 6 が正常に記録されたと判定された場合、ステップ S 58 に進み、管理機能 211 は、デジタル情報販売機能 213 の料金算出機能 231 に、販売するデジタル情報 6 の価格を算出させる。

【0110】ステップ S 59 において、管理機能 211 は、明細印字機能 232 に、ステップ S 58 の処理で算出した販売するデジタル情報 6 の価格を、数字およびバーコードなどで領収書に印刷させる。

【0111】ステップ S 60 において、管理機能 211 は、デジタル情報販売装置 101 の装着部 111 からライセンス管理機能付記録媒体 102-1 を排出させる。

【0112】ステップ S 61 において、管理機能 211 は、料金回収機能 233 に、販売するデジタル情報 6 の価格に対応する、支払われた料金を受け取らせ、処理は終了する。

【0113】ステップ S 53 において、ライセンス管理機能付記録媒体 102-1 が認証されないと判定された場合、ライセンス管理機能付記録媒体 102-1 が正当

ではないので、ステップ S 62 に進み、管理機能 211 は、表示部 126 に認証されなかった旨を示すエラーメッセージを表示させ、処理は終了する。

【0114】ステップ S 55 において、販売するデジタル情報 6 が決定されず、中止が要求されたと判定された場合、ステップ S 63 に進み、管理機能 211 は、表示部 126 に処理が中断された旨を示すメッセージを表示させ、処理は終了する。

【0115】ステップ S 57 において、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 102-1 にデジタル情報 6 が正常に記録されないと判定された場合、ステップ S 64 に進み、管理機能 211 は、表示部 126 に書き込みが失敗した旨を示すエラーメッセージを表示させ、処理は終了する。

【0116】このように、デジタル情報販売装置 101 のデジタル情報 6 の販売の他の処理によっても、デジタル情報販売装置 101 は、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 102-1 にデジタル情報 6 を記録させることができる。

【0117】なお、ステップ S 61 の処理において、料金回収機能 233 が、販売するデジタル情報 6 の価格に対応する料金を受け取ると説明したが、購入者に、デジタル情報販売装置 101 が設置されている販売店の金銭の支払いをする場所で、ステップ S 59 の処理で印刷された、販売するデジタル情報 6 の価格を基に、料金を支払わせるようにしてもよい。

【0118】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【0119】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図 3 に示すように、磁気ディスク 161 (フロッピディスクを含む)、光ディスク 162 (CD-ROM (Compact Disc-Read Only Memory)、DVD (Digital Versatile Disc) を含む)、光磁気ディスク 163 (MD (Mini-Disc) を含む)、若しくは半導体メモリ 164 などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納される ROM 122 や、記録部 129 を構成するハードディスクなどにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じてルータ、モデムなどの通信部 128 を介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

10

20

30

40

50

【0120】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0121】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0122】

【発明の効果】請求項1に記載の情報販売装置、請求項7に記載の情報販売方法、および請求項8に記載のプログラム格納媒体によれば、販売する情報が蓄積され、情報に対応する利用条件が生成され、情報が暗号化され、暗号化された情報を復号する暗号鍵が生成され、装着されている記録媒体が認証され、認証された記録媒体に、暗号化された情報が利用条件および暗号鍵と共に書き込まれるようにしたので、販売した情報の不正な利用の防止ができるようになる。

【図面の簡単な説明】

【図1】従来のデジタル情報販売システムの構成を説明する図である。

【図2】本発明に係るデジタル情報販売システムの一実施の形態を説明する図である。

【図3】デジタル情報販売装置101の構成の例を説明する図である。

*【図4】本発明に係るデジタル情報販売システムの一実施の形態の構成を説明する図である。

【図5】利用条件およびデジタル情報鍵が付加されたデジタル情報6を説明する図である。

【図6】デジタル情報販売装置101のデジタル情報6の販売の処理を説明するフローチャートである。

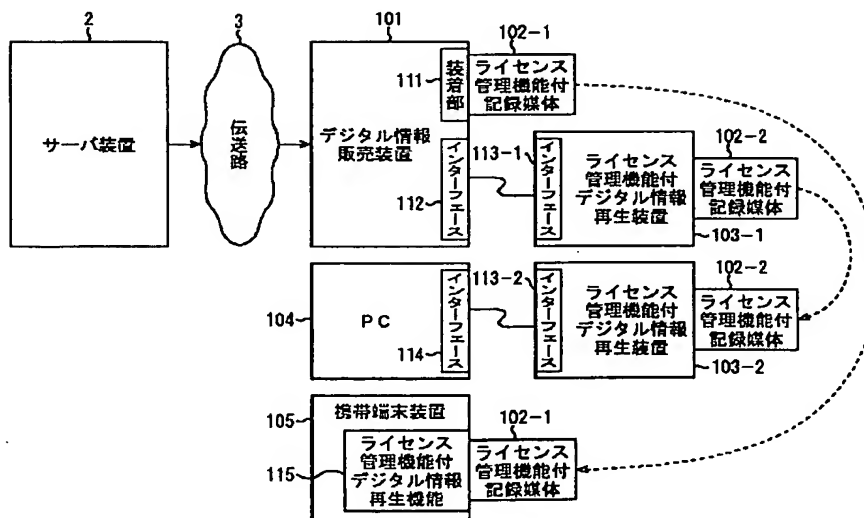
【図7】デジタル情報販売装置101の認証機能214とライセンス管理機能付記録媒体102-1との認証の処理を説明する図である。

【図8】デジタル情報販売装置101のデジタル情報6の販売の他の処理を説明するフローチャートである。

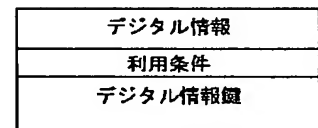
【符号の説明】

101 デジタル情報販売装置, 102-1, 102-2 ライセンス管理機能付記録媒体, 103-1, 103-2 ライセンス管理機能付デジタル情報再生装置, 112 インターフェース, 121 CPU, 122 ROM, 123 RAM, 128 通信部, 129 記録部, 131 書き込み部, 132 料金回収部, 161 磁気ディスク, 162 光ディスク, 163 光磁気ディスク, 164 半導体メモリ, 211 管理機能, 212 デジタル情報蓄積機能, 213 デジタル情報販売機能, 214 認証機能, 227 ライセンス生成機能, 228 デジタル情報鍵生成機能, 229 暗号化機能, 230 ライセンス付デジタル情報書き込み機能

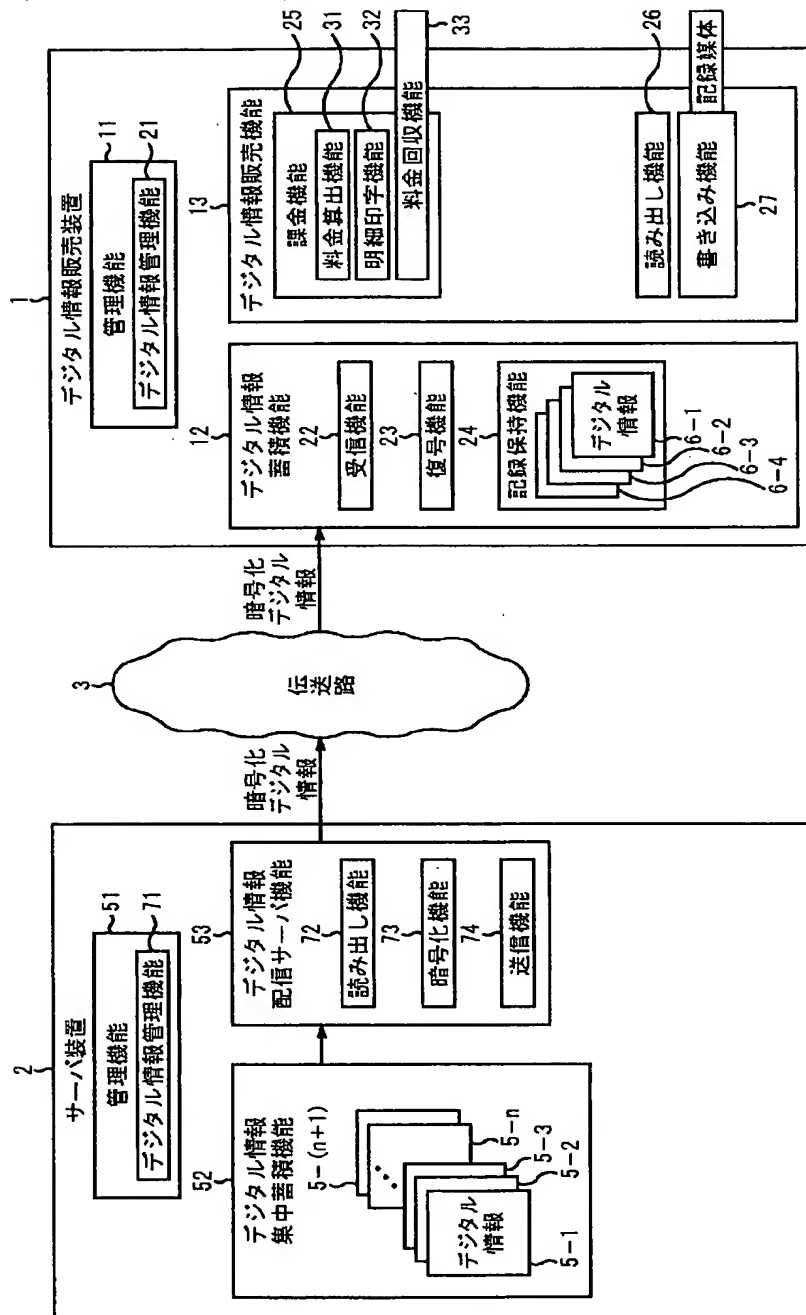
【図2】



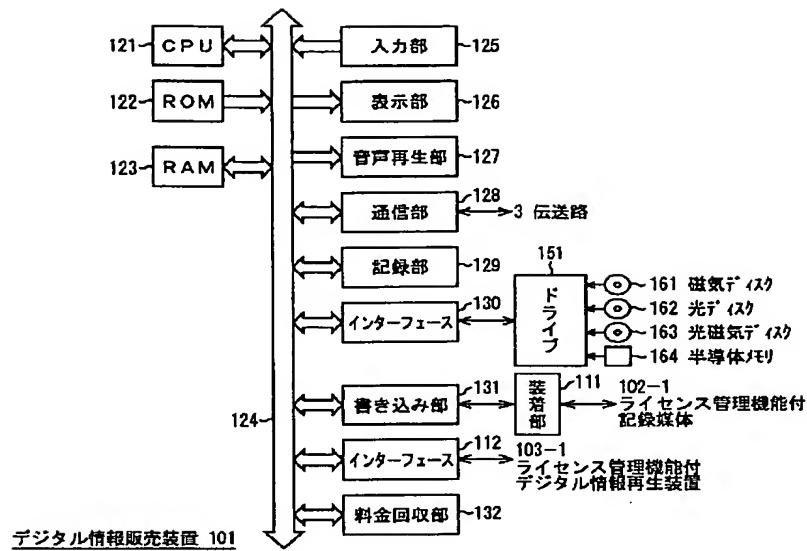
【図5】



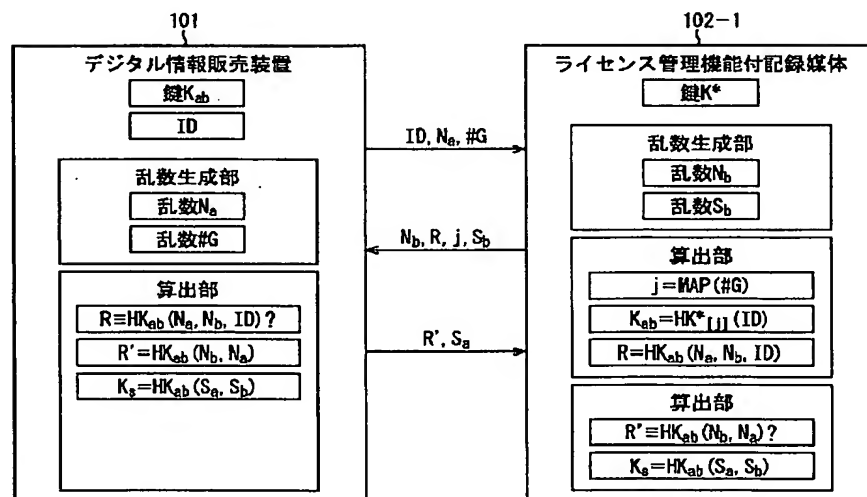
【図1】



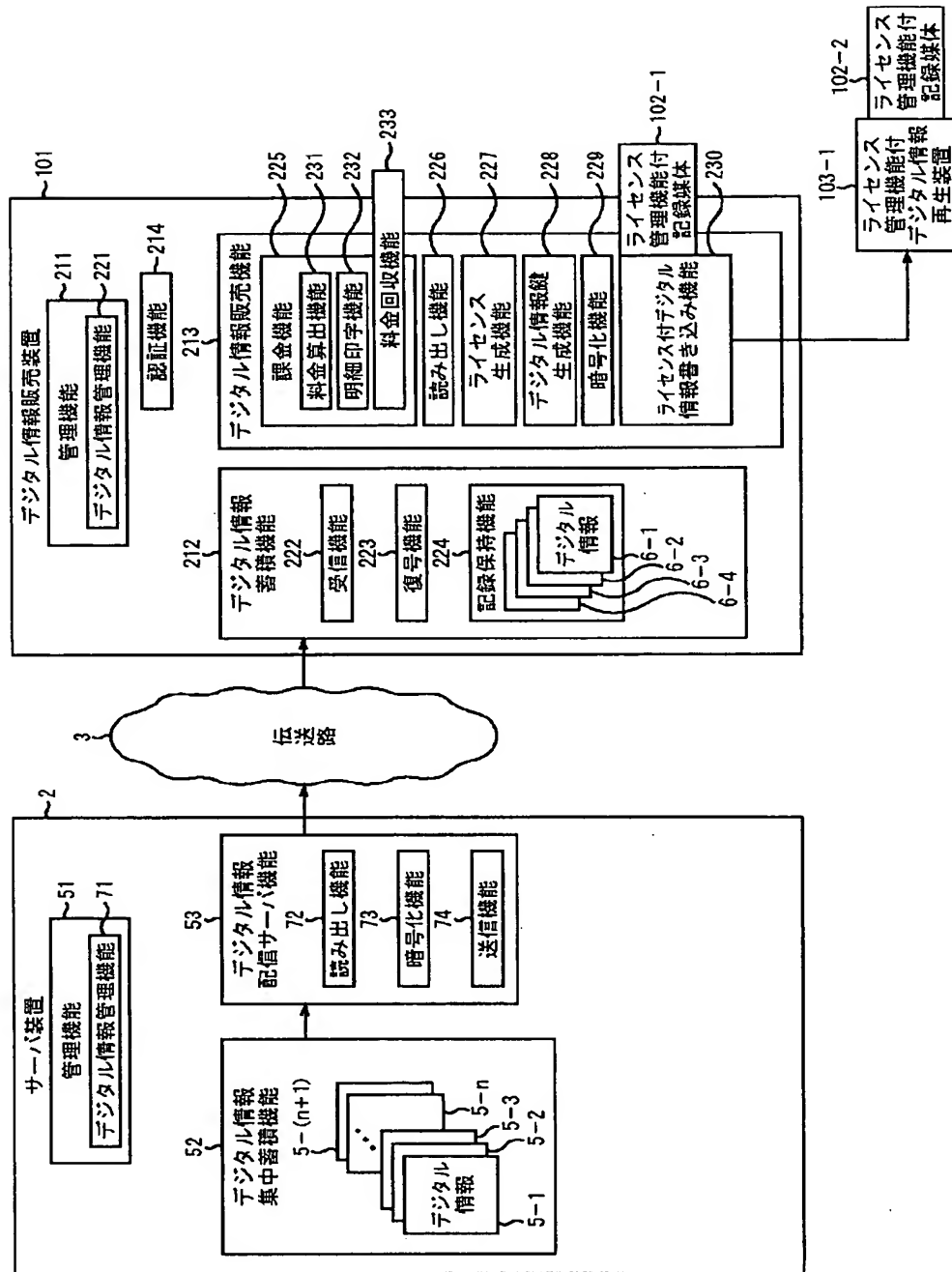
【図3】



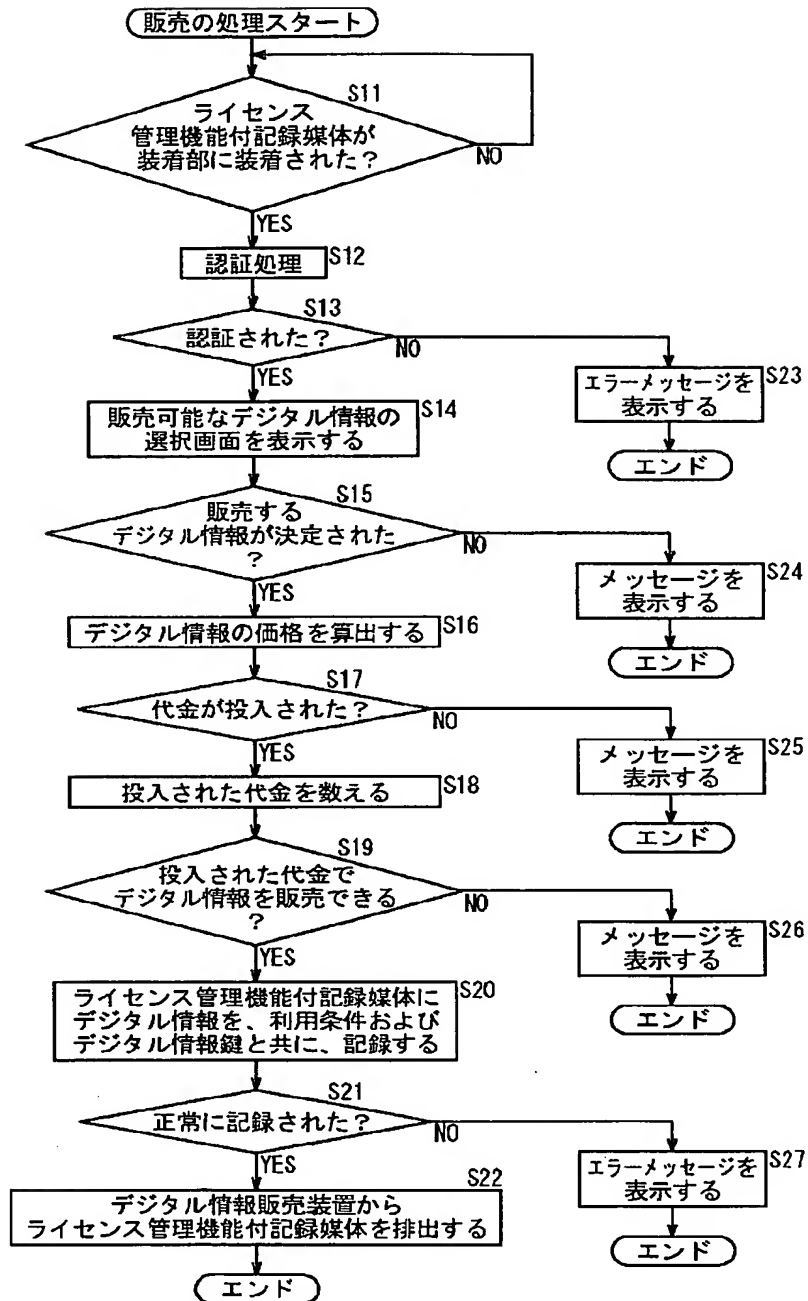
【図7】



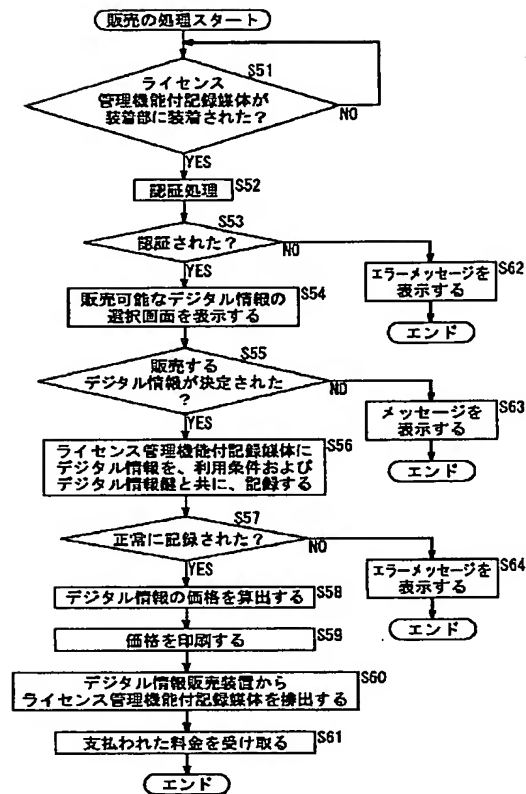
【図4】



【図6】



【図8】



フロントページの続き

(51)Int.Cl.⁷

H 0 4 L 9/32

H 0 4 N 7/16

識別記号

F I

H 0 4 N 7/16

H 0 4 L 9/00

ターマコード(参考)

Z

6 7 3 B

Fターム(参考) 5B049 BB00 GG02 GG10

5C064 BA01 BA07 BB05 BB10 BC10

BC17 BC22 BC25 BD02 BD07

BD14

5D044 AB02 AB05 AB07 BC01 BC04

CC04 DE50 EF05 FG18 GK17

HL02 HL04 HL08

5J104 AA01 AA07 AA16 EA04 EA16

KA02 KA06 NA02 PA10 PA14